CLAIMS

[c1] 1. A decryption system comprising:

a decryption unit for decrypting encrypted program signals using a program decryption key;

a receiver for receiving signals including encrypted data defining the program decryption key;

a security processor; and

an interface providing a first path for transferring the encrypted data from the receiver to the security processor and providing a second path, separate and independent of the first path, for transferring data from the security processor to the decryption unit;

and wherein the security processor is configured to decrypt the encrypted data using a program key so as to extract the program decryption key from the encrypted data, and to output the program decryption key for transfer through the second path of the interface to the decryption unit.

[c2] 2. A system as claimed in claim 1, wherein the encrypted program signals include encrypted video signals and encrypted audio signals, the decryption unit comprises a video decryption unit for decrypting the encrypted video signals and an audio decryption unit for decrypting the encrypted audio signals, the encrypted data defines both a video working key and an audio working key, and the security processor is configured to extract both the video and the audio working keys from the encrypted data.

[c3] 3. A system as claimed in claim 1, wherein the security processor is removable.

[c4] 4. A system as claimed in claim 3, wherein the security processor comprises a smart card.

[c5] 5. A system as claimed in claim 3, wherein the security processor is configured for operation by a program downloaded from the receiver after the security processor is connected to the system.

[c6] 6. A system as claimed in claim 5, wherein the downloaded program comprises an applet and data representing the program key.

[c7] 7. A system as claimed in claim 6, wherein the data representing the program key is downloaded in encrypted form and, once downloaded, is decrypted by the applet.

[c8] 8. A system as claimed in claim 1, wherein the signals received by the receiver include data identifying the auditorium in which the working decryption key is authorized to be used, the system further comprising a control processor responsive to the data for controlling the decryption unit.

[c9] 9. A system as claimed in claim 1, wherein the signals received by the receiver include data identifying the time at which the working key is authorized to be used, the system further comprising a control processor responsive to the data for controlling the decryption unit.

[c10] 10. A system as claimed in claim 2, wherein the signals received by the receiver include data identifying a start frame in the video signals at which the working key shall begin to be used, the system further comprising a control processor responsive to the data for controlling the decryption unit.

[c11] 11. A system as claimed in Claim 1, wherein the security processor does not access the program decryption key in decrypted form.

[c12] 12. An apparatus for decrypting encrypted program signals, the apparatus comprising:

receiving means for receiving encrypted key signals containing data defining a working decryption key;

means for transferring the encrypted key signals via a first interface;

first means, connected to the first interface, for decrypting the encrypted key signals, using a program key in a decryption algorithm, to determine the working decryption key;

means for transferring the working decryption key via a second interface, different and operationally separate from the first interface; and

second means, connected to the second interface, for decrypting the encrypted program signals using the working decryption key,

and wherein the decryption algorithm is supplied together with the program decryption key via the receiving means and is downloaded therefrom to the first means for decrypting.

[c13] 13. An apparatus as claimed in claim 12, wherein the encrypted program signals include encrypted video signals and encrypted audio signals, the second means comprises video decrypting means for decrypting the encrypted video signals and audio decrypting means for decrypting the encrypted audio signals, the encrypted key signals define both a video working key and an audio working key, and the first means is configured to extract both the video and the audio working keys from the encrypted key signals.

[c14] 14. An apparatus as claimed in claim 12, wherein the first means comprises a removable smart card.

[c15] 15. An apparatus as claimed in claim 14, wherein the smart card is configured for operation by a program downloaded from the receiver after the smart card is connected to the system.

[c16] 16. An apparatus as claimed in claim 15, wherein the downloaded program comprises an applet and data representing the program key.

[c17] 17. An apparatus as claimed in claim 12, wherein the signals received by the receiving means include data identifying an auditorium in which the working decryption key is authorized to be used, the system further comprising controlling means responsive to the data for controlling the decryption unit.

[c18] 18. An apparatus as claimed in claim 12, wherein the signals received by the receiver include data identifying a time at which the working key is authorized to

be used, the system further comprising controlling means responsive to the data for controlling the decryption unit.

[c19] 19. An apparatus as claimed in claim 13, wherein the signals received by the receiving means include data identifying a start frame in the video signals at which the working key shall begin to be used, the system further comprising controlling means responsive to the data for controlling the decryption unit.

[c20] 20. An apparatus as claimed in claim 12, wherein the decrypted program signals cannot be accessed from the first interface.

[c21] 21. An apparatus in which, initially, a decryption algorithm received by a control processor is passed via a first interface path to a decryption processor where it is installed together with a program decryption key extracted therefrom, and, subsequently, encrypted working decryption keys received by the control processor are passed on to the decryption processor over the first interface path at which decryption processor they are decrypted using the program decryption key to obtain working decryption keys that are then transferred via a second interface path to decryptors for use in decrypting encrypted program signals input to the decryptors.

[c22] 22. A method for installing a decryption key, in which, initially, a decryption algorithm received by a control processor is passed via a first interface path to a decryption processor where it is installed together with a program decryption key extracted therefrom, and, subsequently, encrypted working decryption keys received by the control processor are passed on to the decryption processor over the first interface path at which decryption processor they are decrypted using the program decryption key to obtain working decryption keys that are then transferred via a second interface path to decryptors for use in decrypting encrypted program signals input to the decryptors.

[c23] 23. A method for installing a decryption key, the method comprising:
receiving signals including encrypted data defining a working decryption key;
transferring the encrypted data over a first path to a security processor;

decrypting the encrypted data at the security processor using a program key so as to extract the working decryption key from the encrypted data;

outputting the working decryption key for transfer over a second path, separate and independent of the first path, to a decryption unit; and

decrypting encrypted program signals in a decryption unit using the working decryption key.

[c24] 24. A method as claimed in claim 23, wherein the encrypted program signals include encrypted video signals and encrypted audio signals, and the encrypted data defines both a video working key and an audio working key, the method comprising the decryption unit comprises:

decrypting the encrypted video signals in a video decryption unit;

decrypting the encrypted audio signals in an audio decryption unit; and

extracting both the video and the audio working keys from the encrypted data.

[c25] 25. A method as claimed in claim 23, wherein the security processor is removable.

[c26] 26. A method as claimed in claim 25, wherein the security processor comprises a smart card.

[c27] 27. A method as claimed in claim 23, further comprising connecting the security processor to the system; and

downloading a program to the processor.

[c28] 28. A method as claimed in claim 27, wherein the downloaded program comprises an applet and data representing the program key.

[c29] 29. A method as claimed in claim 28, wherein the data representing the program key is downloaded in encrypted form and, once downloaded, is decrypted by the applet.

[c30] 30. A method as claimed in claim 23, wherein the received signals include data identifying an auditorium in which the working decryption key is authorized to

be used, the method further comprising controlling the decryption unit in response to the data.

[c31] 31. A method as claimed in claim 23, wherein the received signals include data identifying the time at which the working key is authorized to be used, the method further comprising controlling the decryption unit in response to the data.

[c32] 32. A method as claimed in claim 24, wherein the received signals include data identifying a start frame in the video signals at which the working key shall begin to be used, the method further comprising controlling the decryption unit in response to the data.

[c33] 33. A method for decrypting encrypted program signals, the method comprising:

receiving encrypted key signals containing data defining a working decryption key;

transferring the encrypted key signals via a first interface;

decrypting the encrypted key signals, using a program key in a decryption algorithm, to determine the working decryption key;

transferring the working decryption key via a second interface, different and operationally separate from the first interface; and

decrypting the encrypted program signals using the working decryption key,

and wherein the decryption algorithm is supplied together with the program decryption key through the receiving means and is downloaded therefrom to the first means for decrypting.

[c34] 34. A method as claimed in claim 33, wherein the encrypted program signals include encrypted video signals and encrypted audio signals, and the encrypted key signals define both a video working key and an audio working key, the method further comprising:

extracting both the video and the audio working keys from the encrypted key signals

decrypting the encrypted video signals; and

decrypting the encrypted audio signals.

[c35] 35. A method as claimed in claim 33, wherein the decrypting of the encrypted key signals is done by a removable smart card.

[c36] 36. A method as claimed in claim 35, further comprising downloading to the smart card a program for the decrypting of the encrypted key signals.

[c37] 37. A method as claimed in claim 36, wherein the downloaded program comprises an applet and data representing the program key.

[c38] 38. A method as claimed in claim 33, wherein the signals received by the receiving means include data identifying an auditorium in which the working decryption key is authorized to be used, the method further comprising controlling the decryption unit in response to the data.

[c39] 39. A method as claimed in claim 33, wherein the signals received by the receiver include data identifying a time at which the working key is authorized to be used, the method further comprising controlling the decryption unit in response to the data.

[c40] 40. A method as claimed in claim 34, wherein the signals received by the receiving means include data identifying a start frame in the video signals at which the working key shall begin to be used, the method further comprising controlling the decryption unit in response to the data.

[c41] 41. A method as claimed in claim 31, wherein the decrypted program signals cannot be accessed through the first interface.